Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A system comprising:

at least a first input mechanism to receive first multi-factor authentication data associated with Z authentication factors of Z different types~~, the Z types of authentication data are each different~~;

a cryptographic engine to encrypt the first multi-factor authentication data;

a separated user authentication, non-volatile data store to store the encrypted first multi-factor authentication data, the separated user authentication, non-volatile data store accessible only in conjunction with multi-factor user authentication activities;

a first processing unit to determine whether second multi-factor authentication data received via the at least first input mechanism matches a subset of the first multi-factor authentication data, the second multi-factor authentication data associated with N authentication factors of N different types where N is less than Z and greater than one;

the first processing unit to authenticate using the second multi-factor authentication data comprising the subset of the stored first multi-factor authentication data where less than Z authentication factors are available for authentication,~~; and~~ a user being authenticated if the second authentication data matches the subset of the first authentication data.

2. (Original) The system of claim 1 wherein the first input mechanism includes at least one biometric input mechanism.

3. (Original) The system of claim 1 further including

a Trusted Platform Module, the cryptographic engine being included in the

Trusted Platform Module.

4. (Original) The system of claim 1 wherein the first processing unit is one of a microprocessor, a digital signal processor, and an embedded processor.

5. (Original) The system of claim 4 wherein the first processing unit implements a security technology to provide for protected execution.

6. (Original) The system of claim 4 further including a second processing unit separate from the first processing unit.

7. (Currently Amended) A system comprising:

a first processor to execute instructions;

a first non-volatile memory to store instructions to be executed by the processor;

a bus coupled to the processor and the first non-volatile memory to communicate information; and

a user authentication sub-system coupled to the bus, the user authentication sub-system including:

a user authentication input module to receive first multi-factor user authentication data of Z different types~~, the Z types of authentication data are each different~~;

a second, separated non-volatile memory to store an encrypted version of the first multi-factor user authentication data, the second non-volatile memory accessible only in conjunction with multi-factor user authentication activities;

a second user-authentication processor to determine whether second multi-factor user authentication data matches at least a corresponding subset of the first multi-factor user authentication data, the second multi-factor user authentication data including authentication data of N different types, where N is less than Z and greater than one; and

the second user-authentication processor to authenticate using the second multi-factor user authentication data corresponding to the subset of the first multi-factor user authentication data where less than Z authentication factors are available for authentication, a user being authenticated if the second authentication data matches the subset of the first authentication data.

8. (Original) The system of claim 7 wherein the user authentication sub-system further includes

a cryptographic engine to encrypt the first user authentication data prior to storage.

9. (Previously Presented) The system of claim 8 wherein the cryptographic engine is included in a Trusted Platform Module.

10. (Previously Presented) The system of claim 7 wherein the user authentication input module is to receive first multi-factor authentication data including at least one biometric authentication factor.

11. (Canceled)

12. (Original) The system of claim 7 wherein the second non-volatile memory is physically separated from the first non-volatile memory.

13. (Original) The system of claim 7 wherein the second non-volatile memory is logically separated from the first non-volatile memory.

14. (Currently Amended) A method comprising:

receiving first multi-factor authentication data at a user-authentication sub-system, the first multi-factor authentication data including Z different types of authentication data~~, the Z types of authentication data are each different~~;

decrypting second multi-factor authentication data stored in a separated non-volatile memory accessible only in conjunction with multi-factor user authentication activities, the second multi-factor authentication data including N different types of authentication data where N is less than Z and greater than one;

determining whether the second multi-factor authentication data matches at least a corresponding subset of the first multi-factor authentication data; and

authenticating using the second multi-factor authentication corresponding to the subset of the first multi-factor authentication data where less than Z authentication factors are available for authentication, a user being authenticated if the second authentication data matches the subset of the first authentication data.

15. (Original) The method of claim 14 further comprising:

granting access to a resource if the first multi-factor authentication data matches at least a corresponding subset of the second multi-factor authentication data; and

denying access to the resource if the first multi-factor authentication data does not match at least a corresponding subset of the second multi-factor authentication data.

16. (Original) The method of claim 15 further comprising:

requesting the first multi-factor authentication data in response to an attempt to access the resource.

17. (Original) The method of claim 14 wherein receiving first multi-factor authentication data includes receiving at least one biometric data input type.

18. (Original) The method of claim 14 further comprising receiving the second multi-factor authentication data;

encrypting the second multi-factor authentication data; and

storing the second multi-factor authentication data in the separated, non-volatile memory.

19. (Original) The method of claim 14 wherein

determining whether the first multi-factor authentication data matches at least a corresponding subset of the second multi-factor authentication data includes using an authentication processor separate from a main processor.

20. (Withdrawn) A method comprising:

generating at a requestor a request to authenticate a user;

performing a bi-lateral authentication process to bi-laterally authenticate a user authentication sub-system and the requestor; and

authenticating a user with the user authentication sub-system prior to granting access to a resource if the sub-system and the requestor are bi-laterally authenticated.

21. (Withdrawn) The method of claim 20 wherein performing the bi-lateral authentication process includes exchanging data encrypted with previously exchanged keys.

22. (Withdrawn) The method of claim 20 wherein authenticating a user with the user authentication sub-system includes authenticating a user with an operating system-independent user authentication sub-system.

23. (Withdrawn) A method comprising:

in response to receiving a request for user authentication, checking a platform configuration register to determine if a platform configuration has changed since a previous time the platform configuration register was checked;
and

performing a user authentication process with a user authentication sub-system only if it is determined that the platform configuration has not changed.

24. (Withdrawn) The method of claim 23 wherein performing the user authentication process with the user authentication sub-system includes

receiving first multi-factor authentication data at the user authentication sub-system;

decrypting second multi-factor authentication stored in a separated nonvolatile memory; and

determining whether the first multi-factor authentication data matches at least a corresponding subset of the second multi-factor authentication data.

25. (Withdrawn) The method of claim 24 wherein receiving first multi-factor authentication data includes receiving at least one biometric data type.

26. (Withdrawn) The method of claim 24 further comprising

controlling access to a resource based on whether the first multi-factor authentication data matches at least a corresponding subset of the second multifactor authentication data.

27. (Withdrawn) The method of claim 26 wherein controlling access to a resource includes controlling access to at least one of an enterprise resource, an application and a computer system.

28. (Currently Amended) A tangible machine-accessible storage medium storing data that, when accessed by a machine, causes the machine to perform a method including:

requesting an autonomous user authentication sub-system to perform a user authentication process;

requesting a user to provide first multi-factor authentication data including Z <u>different</u> types of authentication data~~, the Z types of authentication data are each different~~;

determining whether to grant access to a resource based on whether the

user authentication sub-system determines that a second multi-factor authentication data matches at least a corresponding subset of first multi-factor authentication data encrypted and stored in a separated non-volatile memory of the sub-system accessible only in conjunction with multi-factor user authentication activities, the second multi-factor authentication data including N different types of authentication data, where N is less than Z and greater than one; and

authenticating using the second multi-factor authentication data corresponding to the subset of the first multi-factor authentication data where less than Z authentication factors are available for authentication, a user being authenticated if the second authentication data matches the subset of the first authentication data.

29. (Previously Presented) The tangible machine-accessible storage medium of claim 28 wherein requesting the user to provide first multi-factor authentication data includes requesting at least one biometric input data type.